IN THE CLAIMS

Please add claims 36-59 as follows:

36. The method of claim 1, wherein the elliptic curve is over a finite field;

the finite field is represented by a field polynomial; and

the field polynomial is of low hamming weight.

37. The method of claim 36, wherein the field polynomial is selected from a binomial, a trinomial, and a pentanomial.

a'

38. The method of claim 1, wherein the elliptic curve is over a finite field and the finite field is represented as a field tower.

39. The method of claim 38, wherein the field tower comprises an outer field; and

the extension degree of the outer field is selected from the numbers 2, 3, 5, a product of the numbers, or repeated uses of any of the numbers.

40. The method of claim 38, wherein the field tower has more than two levels.

41. The method of claim 38, wherein the field tower comprises an inner field, having arithmetic, and wherein the arithmetic is accelerated by using pre-computed tables for operations selected from the group consisting of multiplication, squaring, taking the square root, division, reciprocation, taking the logarithm, exponentiation, calculating solutions of quadratic equations, and calculating the solutions of polynomial equations.

42. The method of claim 1, wherein the point modification algorithm comprises solving a quadratic equation using an efficient algorithm.

43. The method of claim 1, wherein the point modification algorithm comprises computing a reciprocal of a field element using an efficient algorithm.

44. The method of claim 1, wherein the point modification algorithm comprises at least one of adding and subtracting of elliptic curve points using an efficient algorithm.

45. The method of claim 44, wherein the addition and subtraction comprises computing a reciprocal of a field element using an efficient algorithm.

46. The method of claim 1, wherein the point modification algorithm comprises point multiplication using a sliding-window method.

47. The method of claim 1, wherein the point modification algorithm comprises at least two occurrences of point fractioning chained together.

48. The method of claim 47, wherein the elliptic curve points comprise intermediate points, having coordinates, and wherein the computation of some of the coordinates is omitted.

49. The method of claim 1, wherein the point modification algorithm further comprises choosing a multiplier having a low hamming weight.

a'

50. The method of claim 1, wherein the point modification algorithm includes point addition and subtraction steps and the point modification algorithm is chosen to minimize the number of steps.

51. The method of claim 1, wherein the point modification algorithm is an addition-subtraction chain, intermixed with point fractioning.

52. The method of claim 1, wherein the elliptic curve is over a finite field, and the size of the finite field is increased such that a smaller number of addition and subtraction steps may be combined with a larger number of point fractioning steps, such that the overall computation effort is reduced, while preserving a specified level of security.

53. The method of claim 42, wherein the efficient algorithm is accelerated by using a Half-Trace formula.

54. The method of claim 42, wherein the efficient algorithm is accelerated by using the relationship between Qsolve(C) and Qsolve (C^2).

55. The method of claim 42, wherein the required storage of the efficient algorithm is reduced by using the relationship between Qsolve(C) and Qsolve(C^2).

56. The method of claim 1, wherein the point modification algorithm further comprises:

using a plurality of representations of the points;

using input points in one or more representations to produce output points in a different representation;

selecting representations that are optimal for succeeding point modification algorithms; and

wherein at least three changes of representation occur.

57. The method of claim 1, wherein at least some of the points are represented in XR representation.

58. The method of claim 56, further comprising switching between the XR and XY representations.

59. A method comprising:

selecting an elliptic curve method;

executing a point modification algorithm to manipulate points of the elliptic curve method, the point modification algorithm comprising one or more ambiguous point triplication steps, where the ambiguity is resolved by determining whether a point is twice halvable;

generating a signal having a distinct characteristic using the elliptic curve method;

providing substantive content; and

manipulating the substantive content using the distinct characteristic.